REMARKS

The Examiner is thanked for the performance of a thorough search.

STATUS OF CLAIMS

Claims 8-10 and 12 have been cancelled.

Claims 1-7, 11, and 13 have been amended.

Claims 14-25 have been added.

No claims have been withdrawn.

Claims 1-7, 11, and 13-25 are currently pending in the application.

SUMMARY OF THE REJECTIONS/OBJECTIONS

Claims 1, 7, 11, and 13 have been objected to based on informalities. Claims 1-6 and 8-10 have been rejected under 35 U.S.C. § 112, second paragraph, as allegedly indefinite. Claim 6 is objected to under 37 CFR 1.75 as being an exact duplicate of Claim 5. Claims 1, 7, and 13 have been provisionally rejected under the judicially-created doctrine of obviousness-type double patenting over Claim 5 of pending application S/N 09/407,785 in view of U.S. Patent Number 6,263,435 B1 issued to Dondeti et al (" *Dondeti* "). Claims 1-13 have been rejected under 35 U.S.C. § 102(e) as allegedly anticipated by *Dondeti*. The rejections are respectfully traversed.

RESPONSE TO REJECTIONS NOT BASED ON THE PRIOR ART

Claims 1, 7, 11, and 13 have been objected to based on informalities. Each of the informalities has been corrected. Thus, the Applicant respectfully submits that the objections to Claim 1, 7, 11, and 13, based on the cited informalities have been traversed.

Claims 1-6 and 8-10 have been rejected under 35 U.S.C. § 112, second paragraph, as allegedly indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 1 has been amended to provide antecedent basis for the term objected to in the Office Action. Claims 8-10 have been cancelled. Thus,

A

the Applicant respectfully submits that the rejections of Claims 1-6 as allegedly indefinite have been traversed and that the rejections of Claims 8-10 are rendered moot.

Claim 6 has been objected to under 37 CFR 1.75 as being an exact duplicate of Claim 5. Claim 6 has been amended so that it is not an exact duplicate of Claim 5. Thus, the Applicant respectfully submits that the objection to Claim 6 as being duplicative of Claim 5 has been traversed.

The Office Action provisionally rejected Claims 1, 7, and 13 under the judicially-created doctrine of obviousness-type double patenting as being unpatentable over Claim 5 of Application 09/407,785 in view of *Dondeti.* The Applicant disagrees with the rejection and believes that the pending claims are clearly patentably distinct from the claims of Application 09/407,785 in view of *Dondeti.* However, to advance prosecution in an expeditious manner, a proper Terminal Disclaimer is timely filed concurrently herewith. The Terminal Disclaimer is sufficient to overcome the double patenting rejection, as noted in the Office Action at page 4. See 37 CFR 1.130(b). In addition, the Applicant provides the following statement of common ownership per MPEP §706.02(l)(2)(II):

> The subject matter of Application 09/470,054 and Application 09/407,785 were, at the time the invention of Application 09/470,054 was made, owned by Cisco Technology, Inc.

Therefore, the Applicant respectfully submits that the terminal disclaimer included herein and the statement of common ownership above traverse the double patenting rejection of Claims 1, 7, and 13.

RESPONSE TO REJECTIONS BASED ON THE PRIOR ART

Claims 1-13 have been rejected under 35 U.S.C. § 102(e) as allegedly anticipated by *Dondeti*. The rejections are respectfully traversed.

A

A. CLAIM 1

Claim 1 features:

> "A method for communicating a session key from a first multicast proxy service node of a secure multicast group to a plurality of other multicast proxy service nodes of the secure multicast group in a communication network, wherein each of the multicast proxy service nodes is capable of establishing multicast communication and serving as a key distribution center, the method comprising the steps of:
>
> creating and **storing an original group session key associated with the secure multicast group *in a first directory***;
>
> authenticating the first multicast proxy service node with a subset of the multicast proxy service nodes that are affected by an addition of the first multicast proxy service node to the secure multicast group, based on the original group session key stored in the first directory;
>
> receiving a plurality of private keys from the subset of the multicast proxy service nodes;
>
> receiving a new group session key for the secure multicast group, for use after addition of the first multicast proxy service node, from **a local multicast proxy service node that has received the original group session key through periodic *replication of the first directory***;
>
> communicating the new group session key to the first multicast proxy service node; and
>
> communicating a message to the subset of the multicast proxy service nodes that causes the subset of the multicast proxy service nodes to update their private keys." (emphasis added).

Thus, Claim 1 features "storing an original group session key associated with the secure multicast group *in a first directory*" and "a local multicast proxy service node that has received the original group session key through periodic *replication of the first directory...*"

A

In other words, in the approach of Claim 1, the local multicast proxy service node obtains the group session key via directory replication.

For example, an embodiment in the Application on page 9, lines 13-18 is described as follows: "Because keys as well as key version information are housed in the directory, multicast security can be achieved over any number of network domains across the entire enterprise. **Key information is stored in**, and the logical tree is supported by, **a directory service. Replication of the directory accomplishes distribution of keys**. Event service nodes may obtain current key information from a local copy of the replicated directory." (emphasis added.)

In contrast, *Dondeti* discloses a "logical tree structure...[that] defines key groups and subgroups, with each subgroup having a subgroup manager. Dual encryption allows the sender of the multicast data to manage distribution of a first set of encryption keys whereas the individual subgroup managers manage the distribution of a second set of encryption key." (Abstract.) In particular, key distribution in *Dondeti* is handled in a conventional manner by sending keys from one member of the multicast to the other members. For example, "Each subgroup manager (SGM) is responsible for generating a secret key and sharing it with all the corresponding subgroup members in a secure fashion." (Col. 4, lines 20-23.) Similarly, "The sender node 12 generates another key that we call the key encrypting key or KEK. Sender node 12 generates a top level KEK for each of the key groups. Sender node 12 also generates a local subgroup key for the top level subgroup 24...These keys are distributed to the multicast members by the sender." (Col. 4, lines 27-34.)

Thus, *Dondeti* merely describes the conventional sharing of keys via messages sent between members of the multicast. *Dondeti* has no disclosure of use of directory replication.

The Office Action states that *Dondeti* discloses "receiving a new group session key for the multicast group, for use after addition of the first multicast proxy service node, from a local multicast proxy service node that has received the group session key through periodic replication of the directory (see column 5, lines 49-55; figure 4, item 70 and step (106); upon adding the new host to its subgroup members' list effectively replicating the member' list of the sender, a local node acting as a subgroup manager SGM changes the subgroup key LS and sends it; see column 7, lines 4-19; where the subgroup members have a replicated directory of key encrypting keys, KEK_1 and KEK_2 used to encrypt a data encrypting key DEK)."

A

However, the portion of *Dondeti* cited in the Office Action describes distributing keys according to a key distribution tree via key distribution packets. Specifically, *Dondeti* states: "the DEKs are distributed via the key distribution tree. We use the key distribution tree in FIG. 2 to illustrate the DEK distribution. The sender generates a key distribution packet...Each of the sender's children decrypts its part of the key distribution packet. Each of them then encrypts its piece of the packet with the subgroup key they manage and multicasts the encrypted DEK to its children. In our example in FIG. 2, P_1 multicasts the encrypted packet..." (Col. 7, lines 2-11).

Thus, *Dondeti* merely discloses key distribution between members via packets that are sent through the multicast in which the responsibility for sharing the keys between members is based on the hierarchical grouping of the members of the multicast. In fact, an electronic search of *Dondeti* reveals that the word "directory" is not even mentioned anywhere in *Dondeti*, nor is the word "replication" or a variant thereof included anywhere in the disclosure of *Dondeti*. There is nothing in *Dondeti* that discloses, teaches, suggests, or in any way renders obvious the distribution of keys through directory replication as featured in Claim 1.

Because *Dondeti* fails to disclose, teach, suggest, or in any way render obvious "storing an original group session key associated with the secure multicast group *in a first directory*" and "a local multicast proxy service node that has received the original group session key through periodic *replication of the first directory...*" as featured in Claim 1, the Applicant respectfully submits that, for at least the reasons stated above, Claim 1 is allowable over the art of record and is in condition for allowance.

B. CLAIMS 7, 11 AND 13

Claims 7, 11, and 13 contain features that are similar to those described above with respect to Claim 1. In particular both Claims 7 and 13 feature "storing an original group session key associated with the secure multicast group *in a first directory*" and "a local multicast proxy service node that has received the original group session key through periodic *replication of the first directory...*," both of which are the same as in Claim 1. Furthermore, Claim 11 features "one of the multicast proxy service nodes generates a first group session key...and distributes the first group session key to other multicast proxy service nodes in the secure multicast or broadcast group using directory replication," which is similar to Claim 1.

+A

Therefore, based on at least the reasons stated above with respect to Claim 1, the Applicant respectfully submits that Claims 7, 11, and 13 are allowable over the art of record and are in condition for allowance.

C. CLAIMS 2-6, 14-18, 19-23, AND 24-25

Claims 2-6, 14-18, 19-23, and 24-25 are dependent upon Claims 1, 13, 7, and 11, respectively, and thus include each and every feature of the corresponding independent claims. Each of Claims 2-6, 14-18, 19-23, and 24-25 is therefore allowable for the reasons given above for Claims 1, 13, 7, and 11. In addition, each of Claims 2-6, 14-18, 19-23, and 24-25 introduces one or more additional limitations that independently render it patentable. However, due to the fundamental differences already identified and in order to expedite the positive resolution of this case, a separate discussion of those limitations is not included at this time. Therefore, it is respectfully submitted that Claims 2-6, 14-18, 19-23, and 24-25 are allowable for the reasons given above with respect to Claims 1, 13, 7, and 11.

CONCLUSION

The Applicant believes that all issues raised in the Office Action have been addressed and that allowance of the pending claims is appropriate. Entry of the amendments and further examination on the merits are respectfully requested.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

A

To the extent necessary to make this reply timely filed, the Applicant petitions for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Craig G. Holmes
Reg. No. 44,770

Date: March 29, 2004

1600 Willow Street
San Jose, CA 95125
Telephone: (408) 414-1080, ext. 207
Facsimile: (408) 414-1076

CERTIFICATE OF MAILING
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Hon. Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

on 3-31-04 by

A